

REMARKS

Following is information requested by the Examiner in the paper mailed January 27, 2004. Such information has been itemized by paragraph per the paper mailed January 27, 2004.

2. The Examiner has requested that applicant identify products and services embodying the disclosed subject matter of the claims, and identify the properties of similar products and services found in the prior art. In response, applicant submits herewith Appendix A including a description of the "Norton Personal Firewall 2003," which is a product embodying the subject matter of applicant's claims. The Examiner should also note that Network Associates' McAfee Personal Firewall also incorporates the claimed subject matter. The properties of similar products/services that are found in the prior art are either unknown or cannot be readily obtained.

3. The Examiner has further requested that applicant provide the names of any products or services that have incorporated the claimed subject matter. Again, in response, applicant submits herewith Appendix A including a description of a product named "Norton Personal Firewall 2003," which has incorporated the claimed subject matter. The Examiner should also note that Network Associates' McAfee Personal Firewall also incorporates the claimed subject matter.

4. The Examiner has further requested a copy of the rigid comparison of the alleged infringing device and method identified in the petition filed on 05/14/03 (paper #4) along with any supporting documents concerning place and date(s) of use and/or sale of the alleged infringing device. In response, applicant submits herewith Appendix B including a claim chart correlating the infringing device and method of Appendix A with the claims of the present application. With respect to the requested supporting documents concerning place and date(s) of use and/or sale of the alleged infringing device, Appendix A indicates that the subject matter relating to the "Norton Personal Firewall 2003" was published on July 25, 2002.

5. The Examiner has still further requested that applicant state the specific improvements of the claimed subject matter in Claims 1, 13 and 25-29 over the disclosed prior art and indicate the specific elements in the claimed subject matter that provide those improvements. In response, following is such claim-by-claim analysis.

Claims 1, 13 and 25-29 provide a technique for tracing a traffic event utilizing a firewall. Shown below in **bold** are selected elements in the claimed subject matter that provide related improvements, when taken in combination.

1. A method for tracing a traffic event utilizing a firewall, comprising:
 - (a) **executing a firewall on a local computer;**
 - (b) **monitoring traffic events between the local computer and a remote computer over a network utilizing the firewall;**
 - (c) **displaying the traffic events utilizing the firewall;**
 - (d) **tracing at least one of the traffic events utilizing the firewall; and**
 - (e) **displaying a map of the trace utilizing the firewall.**

13. A computer program product for tracing a traffic event utilizing a firewall, comprising:
 - (a) computer code for **executing a firewall on a local computer;**
 - (b) computer code for **monitoring traffic events between the local computer and a remote computer over a network utilizing the firewall;**
 - (c) computer code for **displaying the traffic events utilizing the firewall;**
 - (d) computer code for **tracing at least one of the traffic events utilizing the firewall; and**
 - (e) computer code for **displaying a map of the trace utilizing the firewall.**

25. A system for tracing a traffic event utilizing a firewall, comprising:
- (a) logic for **executing a firewall on a local computer;**
 - (b) logic for **monitoring traffic events between the local computer and a remote computer over a network utilizing the firewall;**
 - (c) logic for **displaying the traffic events utilizing the firewall;**
 - (d) logic for **tracing at least one of the traffic events utilizing the firewall;** and
 - (e) logic for **displaying a map of the trace utilizing the firewall.**
26. A method for tracing a traffic event utilizing a firewall, comprising:
- (a) **executing a firewall on a local computer;**
 - (b) **monitoring traffic events between the local computer and a remote computer over a network utilizing the firewall;**
 - (c) **displaying the traffic events utilizing the firewall;**
 - (d) **tracing at least one of the traffic events utilizing the firewall;**
 - (e) **displaying a geographical location of a plurality of network segments associated with the traffic event upon the selection of a first one of a plurality of views utilizing the firewall;**
 - (f) **displaying a plurality of nodes of the network segments upon the selection of a second one of the views utilizing the firewall;** and
 - (g) **displaying a list of the network segments upon the selection of a third one of the views utilizing the firewall.**
27. A method for tracing a traffic event utilizing a firewall, comprising:
- (a) **executing a firewall on a local computer;**
 - (b) **monitoring traffic events between the local computer and a remote computer over a network utilizing the firewall;**
 - (c) **logging the traffic events in an event log utilizing the firewall, wherein the event log identifies a time and an Internet Protocol (IP) address associated with the traffic events;**

- (d) **organizing the traffic events in the event log based on times the traffic events are logged utilizing the firewall;**
- (e) **displaying the traffic events in the event log utilizing the firewall;**
- (f) **detecting the selection of one of the traffic event by a user;**
- (g) **tracing at least one of the traffic events utilizing the firewall upon the selection thereof, wherein the tracing identifies a plurality of network segments traversed by the traffic event;**
- (h) **detecting the selection of one of a plurality of views by the user; and**
- (i) **displaying the network segments in the selected view upon the selection of one of the views.**

28. A method for geographically tracing a traffic event utilizing a personal firewall, comprising:

monitoring traffic events between a local computer and a remote computer over a network utilizing a personal firewall;

displaying the traffic events in an event log utilizing the personal firewall, wherein the traffic events are organized based on a time associated therewith;

tracing at least one of the traffic events utilizing the personal firewall; and

displaying a geographical map of the trace utilizing the personal firewall,

wherein the at least one traffic event is traced in response to a user request.

29. A computer program product for geographically tracing a traffic event utilizing a personal firewall, comprising:

computer code for monitoring traffic events between a local computer and a remote computer over a network utilizing a personal firewall;

computer code for displaying the traffic events in an event log utilizing the personal firewall, wherein the traffic events are organized based on a time associated therewith;

computer code for **tracing at least one of the traffic events utilizing the personal firewall**; and
computer code for **displaying a geographical map of the trace utilizing the personal firewall**,
wherein the at least one traffic event is traced in response to a user request.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. Applicants are enclosing a check to pay for the added claims. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P094_02.013.01).

Respectfully submitted,
Silicon Valley IP Group


Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100